SECRET

"Payne Panel

MARTIN MARIETTA AEROSPACE

ORLANDO DIVISION
POST OFFICE BOX 5837
ORLANDO, FLORIDA 32805
TELEPHONE (305) 855-6100, EXT. 2007

FRED A. PAYNE
VICE PRESIDENT AND CHIEF ENGINEER

January 3, 1973

073-73

MEMORANDUM FOR DSB TASK FORCE ON TACTICAL WARNING/ATTACK ASSESSMENT

SUBJECT: DRAFT REPORT

The attached draft of the final report of our DSB Task Force on TW/AA is for your final editing and comments. As many of you know, the current plan is to brief the report to the C^3/I panel on the 9th of January and, subject to their approval, to the main DSB on the 11th of January, after which there would remain only final publication of the report.

Assuming that all goes as per plan, I will give you a call after the meeting and pass on whatever appears pertinent.

Fred A. Payne
Chairman

Enclosure: Doc. #73-79003

Distribution:
Dr. Davis B. Bobrow
Mr. Robert R. Everett
Gen. James Ferguson
Mr. A. Carl Haussmann, Jr.
Dr. David E. Mann
Dr. Dominic A. Paolucci
Dr. Joseph F. Shea
✓Dr. Donald H. Steininger
Dr. Lloyd H. Wilson
Lt. Col. Norman W. Sparks

WHEN ENCLOSURES ARE WITHDRAWN, THE CLASSIFICATION OF THIS DOCUMENT IS DOWNGRADED TO UNCLASSIFIED.

SECRET

Martin Marietta Aerospace
Orlando Division
P. O. Box 5837
Orlando, Fla. 32805

DRAFT

Document #: 73-79003

Copy #: 8

FINAL REPORT

OF THE

DEFENSE SCIENCE BOARD TASK FORCE

ON

TACTICAL WARNING/ATTACK ASSESSMENT (U)

January 3, 1973

DRAFT

January 3, 1973

MEMORANDUM FOR THE CHAIRMAN, DEFENSE SCIENCE BOARD

SUBJECT: Final Report of the Task Force on Tactical Warning/Attack Assessment (U)

I am pleased to submit to you the attached copies of the final report of subject Task Force. The report is in response to the Charter (Attachment 1) and has been reviewed and approved by the C^3/I Panel of the Defense Science Board.

The report is based on an underlying assumption that the U.S. wants a system which provides national decision makers with very high assurance, real time, data concerning an incoming nuclear attack at a level of detail commensurate with both the time available and remaining options. No document available to the panel explicitly states such an objective, but it seems most reasonable as a basis for conceptual system design.

Some of the recommendations of the report have been recently adopted by the Department of Defense. We have made no attempt to keep the report completely updated as to current activities, but no decision is known to the undersigned which is in basic conflict with the general conclusions of the Task Force.

Acceptance of the reported conclusions should eliminate the need for near-term Defense Science Board review of the attack warning system.

Fred A. Payne
Chairman

CONTENTS

SUMMARY

(S) The currently programmed "tactical" warning net consists of a number of independent sensors and displays designed to detect or track ballistic missiles, aircraft, and submarines during an attack on the CONUS. The addition of central data processing and integrated displays to the tactical warning "net" can create an attack warning "system" which would have much lower false alarm rate than any individual sensor.

(S) The attack warning system can be brought to a high level of reliability and credibility by exercise against peacetime events. The NCA must be fully aware of the possibility of an imminent attack through collateral "all source" data if the information furnished by the attack warning system is to be utilized in a timely fashion.

25X1

(S) It is not possible to harden the attack warning sensors and readout stations against a directed nuclear attack, although they should be hardened against accidental damage. Impact point prediction accuracy and NUDET of the current warning system sensors appears adequate to support NCA decision needs over a wide scale of conceivable attack scenarios.

(S) Recommended development programs for future deployment consideration include improved satellite sensors for SLBM tracking, OTH radars for aircraft and cruise missile tracking, improved undersea surveillance for quiet SSBM tracking, and simulation exercise facilities.

Next 2 Page(s) In Document Exempt

Approved For Release 2004/12/15 : CIA-RDP74J00828R000100080002-1

II. Proposed Attack Warning System

(C) At the present time, each of the attack warning sensor systems is essentially independent with its own processing and display subsystems. The results are brought together at the command post level where correlation of the various warning indications is done by the controller/decision maker on the basis only of the highly aggregated data to which he has ready access.

(C) The reliability and believability of multiple sensor warning data can be greatly increased if two things are done, as illustrated in Figure 2:

1. Tracks, launch points, times, etc., from several sensors are correlated using simple algorithms so that it is possible to say that the sensors are not only providing indications but that those indications are related to the same set of events. Such correlation would greatly reduce the false alarm rate of the total warning system thus increasing what might be called its "real" or intrinsic credibility.

2. The correlated data is then displayed simultaneously to the controllers and decision makers in such a way that they can readily achieve a common understanding of the problem, including what the sensors are indicating, how the indications are correlating and how the indicated situation compares to real world expectations. Such a unified display would increase the "apparent" system credibility, "apparent" in the eyes of the decision makers.

(S) Digital data processing can perform the necessary simple correlation operations and drive an appropriate set of displays. The size of the equipment cannot be accurately predicted until the algorithms are identified, but should be well within the range of existing command post support equipment. One processor could do the entire job, driving displays at all other locations through

communications lines as necessary. At least one duplicate processing facility may be desirable to improve survivability and resistance to accidents. Since the sensor communications now go through single points in most cases, the number and location of warning system processors should probably be decided in the context of a study of the vulnerability of the entire system. Processing stations at NORAD, NMCC, and perhaps SAC appear reasonable. In any event, the basic system (both hardware and software) should be identical in all locations for identical functions to insure that people at all locations are provided with the same information. Similarly, a common unified set of displays should be provided to all users. Modifications to sensor pre-processors and sensor communications may be necessary. (Figure 2)

(S) Steps are already being taken to improve the correlation of warning sensor data at NORAD and elsewhere. Substantial improvements should be possible through evolutionary design and implementation. Additional equipment should be provided when and if necessary. A very rough estimate of the cost of such a processing system at one location including software and logic development, but not including related modifications to sensors, sensor pre-processors, or communications, might be ten to twenty million dollars over several years.

(U) Appendix A contains more detail concerning conceptual system design considerations.

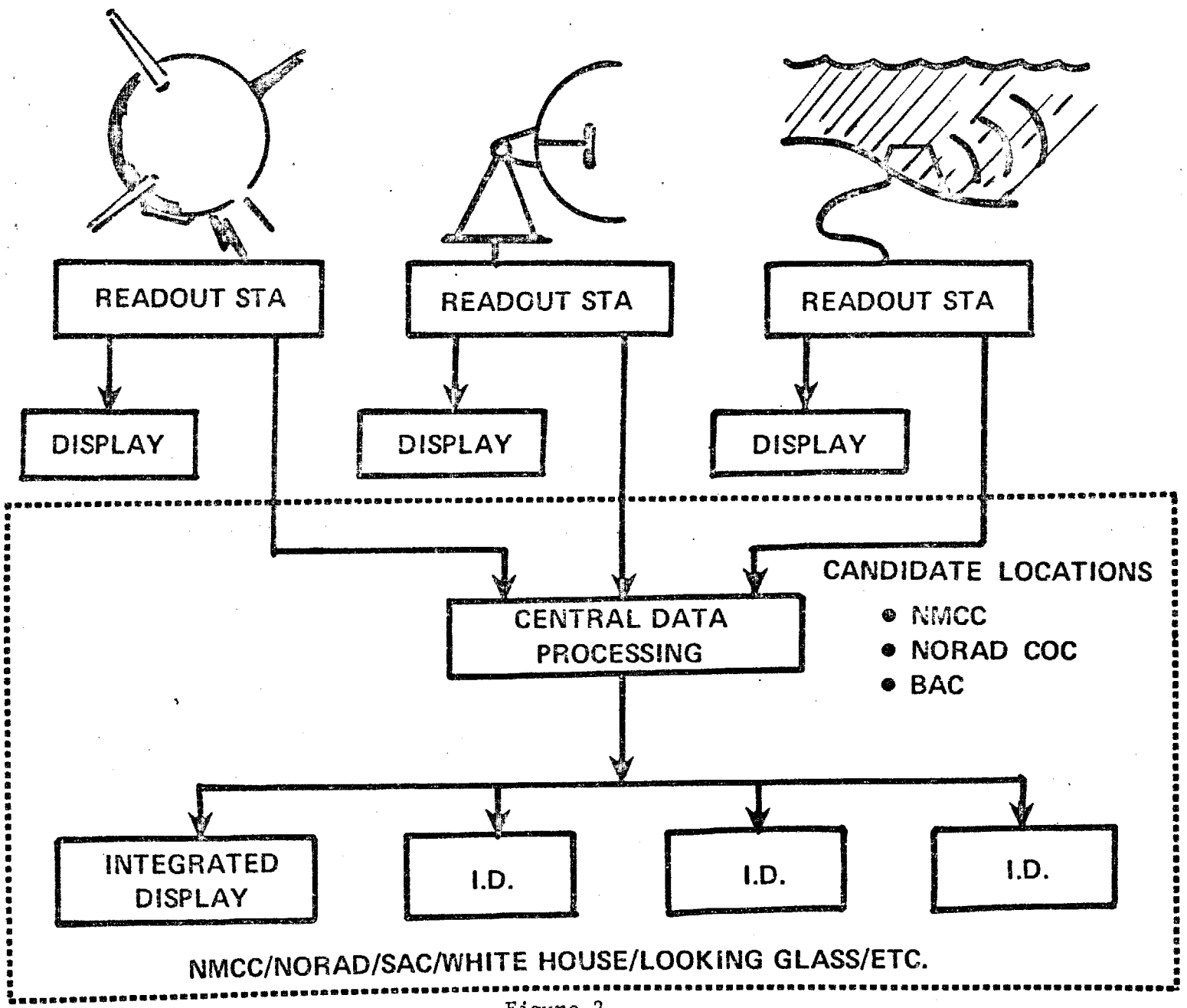

Figure 2.

Approved For Release 2004/12/15 : CIA-RDP74J00828R000100080002-1

III. System Reliability Tests

(U) Effective utilization of the attack warning system will depend on the confidence which can be established in the validity of the events indicated by the system. Analysis alone will not suffice, nor will simulation, even though both are needed.

(S) Although a mass raid will only occur in time of war, sufficient peacetime events, both U.S. and foreign, are available to provide real time readiness listing of the attack warning system using the same phenomenology and, in many instances, the same target vehicles the system is designed to detect. The average number of missile and satellite launches per year is indicated in Figure 3.

(C) The Soviet ICBM and SLBM launches will, in general, exercise the system with single events differing only from the design threat in launch and impact points. The U.S. launches, Soviet satellites, and other launches provide the opportunity to exercise the system over a spectrum of design target characteristics and geographic regions.

(S) The AW system indication of events can be compared to U.S. and intelligence launch records to establish, with high confidence, both the individual sensor launch detection probability and false alarm rate, for single events, the validity and accuracy of the correlation logic, the suitability of the displays, and the overall system detection probability, false alarm rate, attack assessment accuracy, and warning time. Multiple event performance can be estimated from these data, and validated if deemed necessary, by limited multiple launch U.S. experiments.

(C) In a similar fashion, the trans arctic and trans ocean commercial and military aircraft and the peacetime patrols of the U.S. and Soviet nuclear

submarines provide the opportunity to continuously validate the elements of the system involved in A/C and submarine warning.

(C) In summary, the relatively high, continuing incidence of test launches worldwide provides a convenient opportunity to validate and demonstrate the reliability of the integrated attack warning system. The system should be configured to use these events to train the controllers and develop confidence in the system with the decision makers.

WORKING PAPERS

MISSILE/SATELLITE LAUNCHES

EVENT	US	SOVIET	OTHER
SATELLITE	35	90	10
ICBM	40	100	1
SLBM	25	55	7

Figure 3.

IV. Attack Warning System "Credibility"

(S) We have already argued that the addition of appropriate central data processing to the current sensor network can lower the false alarm rate and, through correlation of independently measured data, increase the confidence of the NCA that an indicated attack is real. However, a factor that bears even more heavily on the NCA's willingness to believe an attack indication is his awareness of the state of the world situation at that time. If our relations with the Soviet Union (or other possible attackers) are good and have given no indication of tension, then the NCA will be skeptical of any indication from our warning system that an attack has been launched, and action time provided will likely be wasted in independent verification. If, on the other hand, tensions have been building and particularly, if unusual political and military indicators are present, he will demand less data from the attack warning system before he takes action. Accordingly, the NCA must have already become familiar with the generic type of information provided by the warning system and come to believe in its accuracy and relevance.

(U) As discussed above, it is the function of the attack warning system to give him an accurate display of the indications and false alarm probabilities associated with them. However, it is equally important that the intelligence community provide the necessary mechanisms to keep the NCA continuously up to date on the foreign political and military situation. In this process the NCA must be provided with assessments that cover at least the categories of information shown in Figure 4. Particularly in times of high tension these assessments must reflect current data from all sources which can collect against military strategic warning indicators. Although an evaluation of our current capability

to do this goes beyond purely military information, and hence beyond the purview of this panel, we would like to highlight the importance of this function as an adjunct to the attack warning system.

PRE-ATTACK INDICATORS THAT AFFECT WARNING SYSTEM CREDIBILITY

- POLITICAL ACTIVITY
- FORCE READINESS
- CIVIL DEFENSE READINESS
- CURRENT MILITARY OPERATIONS

Figure 4.

Next 2 Page(s) In Document Exempt

Approved For Release 2004/12/15 : CIA-RDP74J00828R000100080002-1

VI. Attack Warning System Survivability

(S) Current attack warning sensors and readout stations are, in general, quite soft against nuclear attack, and for the most part, their locations are well known. Current and projected technology will not support the hardening of sensor subsystems against the effects of a nearby nuclear explosion. Let us address the useful possibilities which exist between these two extremes. It is desirable that the attack warning components we rely on be hardened to the extent that they are not knocked out accidentally. (An illustration of this unfortunate possibility is the negation of some satellite based functions by a peacetime high altitude test. This scenario actually occurred in the early 1960's.) Sensor and communications hardening technology is readily able to support the hardening of tactical warning units to a level that should preclude any accidental surprises. Hardening technology may be able to permit the reductions of some early warning nuclear vulnerabilities to the extent that enemy action options are not made trivial. That is, the benefit of various levels of nuclear hardening should be compared with the costs to implement various levels of hardening. Thus we could have an indication if there exists a knee in the nuclear hardening cost vs. benefit relationship. Certainly, though, our tactical warning systems should be hardened against unintended nuclear degradations.

(S) It was observed that if the enemy attacks our warning elements he is likely to be successful. We feel that such an attack on our warning system components is highly likely during the initial phases of an assault. The obvious conclusion is, therefore, that there is a low likelihood of a continuing flow of tactical warning sensor information beyond the initial phases of an enemy attack. Such information is, therefore, not likely to be available for any "attack assessment" function which continues beyond the explosion of many nuclear weapons. This fact puts a premium on obtaining information on the basis of tracking

incoming enemy delivery vehicles prior to any substantial number of nuclear detonations. In addition, if there is an ongoing need for "attack assessment" beyond the initial explosions, then sensor systems separate and considerably more specialized than those of our existing warning systems are called for. For example, it is unlikely that a NUDET capability will exist for long as an off-shoot of our tactical warning capability. If NUDET is a requirement it will have to be explicitly addressed. (Figure 6)

(C) In concept, it may be possible to design sensor systems which have a degree of survivability not through being ultra hard, but through a combination of other technical and operation characteristics. As an example, it may be possible to design a satellite which, while performing its mission or while maintaining the capability of performing its mission, has a set of observables which are very difficult to detect, very easy to decoy, or both. Thus, it may be possible to "loose" the satellite in space or in space within a hord of inexpensive decoys. While such concepts are conceivable today they are far from reality and are likely to be expensive. We simply take note of this possibility, but have not addressed a near term utility.

ATTACK WARNING SYSTEM
SURVIVABILITY TO NUCLEAR ATTACK

DIRECT ATTACK – IMPOSSIBLE TO SURVIVE

OTHER EXPLOSIONS – HARDEN TO SURVIVE

POST ATTACK NUDETS – SHOULD BE INDEPENDENT OF ATTACK WARNING SENSORS TO SURVIVE, IF NEEDED

Figure 6.

VII. Attack Assessment System

(S) Attack assessment system requirements vary in important ways depending on the gross size or rate of the attack. Current systems are adequate to provide warning which discriminates between large and small attacks.

(S) Requirements posed by small attacks are for information sufficient to enable the NCA to take revocable actions, e.g., delegate authority, launch bombers, communicate and bargain with attacker. The NCA will seek to make decisions carefully and with considerable deliberation based on an analysis of the intent of the attacker. Was the attack accidental? Who really was the attacker? Was it authorized or unauthorized? With the exception of a direct attack on the NCA, decision time is not extremely limited.

(S) For small attacks, the NCA will ask of the attack assessment system: To whom is the attack attributed? Currently assigned systems can provide an appropriately timely answer for attacks by land-based missiles. They cannot be relied upon to do so for attacks by airplanes or submarines. Existing military capabilities not now assigned to attack assessment could substantially increase our ability to attribute airplane or submarine attacks. Is the attack directed at the NCA? The precision of impact point prediction need only be good enough to answer that question quickly. A few hundred miles CEP is adequate which is within the capability of the current sensor set. If the attack is directed at the NCA, quick decisions are necessary with regard to survival and/or delegation of authority. Has there really been an attack? Of what kind? The NCA will wish to know quickly that nuclear weapons have actually impacted, their numbers and gross types of targets, e.g., military or major population centers). If the DSP survives, timely answers will probably be available. However, DSP survival is not assured nor is there a reliable backup system.

(S) The requirements posed by a large attack are for information sufficient to enable the NCA to take both revocable and irrevocable actions. At a minimum, the NCA must quickly make decisions about delegation of authority and whether to leave bomber launch discretion to CINCSAC. He will also need to have the information to enable him to select a response option. This obviously includes information on the extent to which delay implies the loss of one or several response options.

(S) With regard to the quick choice of an active nuclear response option, only one question is central: Is the attack directed solely at SAC? The current sensor set is capable of providing sufficiently precise and timely impact prediction to answer that question.

(S) Current sensor systems provide sufficient, timely information for delegation of authority decision to be made should the NCA find the information credible and be otherwise prepared and willing to make such decisions.

(S) Finally, verification of the attack in terms of gross size and type of target will be required. The comments made earlier about DSP survivability and the absence of quick-response backup systems also apply to the verification of large attacks.

ATTACK ASSESSMENT SYSTEM

REQUIREMENTS	CURRENTLY MET?
GROSS ATTACK SIZE	YES
IF SMALL ATTACK –	
ATTRIBUTION	POSSIBLY*
LONG DECISION TIME	POSSIBLY*
GROSS IMPACT PREDICTION	YES
SIMPLE ATTACK VERIFICATION	POSSIBLY*
IF LARGE ATTACK –	
SOME FAST DECISIONS	POSSIBLY*
GROSS IMPACT PREDICTION	YES
SIMPLE ATTACK VERIFICATION	POSSIBLY*

*UNDER MANY, BUT NOT ALL, SCENARIOS

Figure 7.

VIII. Research and Development

(S) The USSR has several hundred bombers with intercontinental range and mission. These bombers have exercised with airlaunched cruise missiles of several hundred miles range. A bomber raid which flew at low altitude along the eastern and western coastlines and launched cruise missiles could cover a large fraction of our military and industrial installations. This plausible attack would probably not be detected by current sensors until nuclear detonations have occurred. More speculatively, cruise missiles of similar characteristics could be launched by submarines, and would not be detected either. If the airlaunched cruise missile attack is made coincidentally with ballistic missile attack, the bombers would have taken off many hours before, and it is very possible that we would know they were launched. Under that assumption, naval and air elements such as AWACS could be placed on patrol with reasonable prospects of providing attack warning. If we did not have notice of bomber deployment, or if the cruise missiles were launched from submarines, the option of covering the threat with available operational forces would not exist. Over the horizon backscatter radar has been a candidate for the solution of this problem for some time but serious technical uncertainties still remain. The panel recommends that R&D on OTH-B continue until fundamental performance characteristics and limitations of such radars are better established and can be validated against realistic requirements. Another promising R&D approach to the solution of this problem is surface wave high frequency radar. If it can provide a 500 mi. range, as is possible, the same warning time as against SLBM's would be provided. Technical feasibility and characteristics of such radars is currently under investigation and the panel recommends that this work be continued until system specifications can be confidently projected for possible implementation decision.

Next 1 Page(s) In Document Exempt

Approved For Release 2004/12/15 : CIA-RDP74J00828R000100080002-1

SECRET

WORKING PAPERS

RECOMMENDED R/D PROGRAMS

PROBLEM	APPROACH
IMPROVED BALLISTIC MISSILE TRACKING	SATELLITE SENSORS
OCEANIC BOMBER APPROACH	OTH RADAR
CRUISE MISSILES	OTH RADAR
QUIET SUBMARINES	IMPROVED UNDERSEA SURVEILLANCE
SYSTEM CREDIBILITY & RELEVANCE	EXPERIMENTAL "COMMAND POST" SIMULATIONS

SECRET